文章编号：2095-2163(2023)09-0122-07 中图分类号：TP393 文献标志码：A

基于 SM2 的不动产柜面无纸化签署系统设计与实现

蔡昭炜[1]，刘从军[1,2]，刘 超[3]

（1 江苏科技大学 计算机学院，江苏 镇江 212003；2 江苏科大汇峰科技有限公司，江苏 镇江 212003；
3 镇江市不动产登记交易中心，江苏 镇江 212003）

摘 要：近年来，电子政务的普及带动了不动产业务办理中柜面手工文书签署方式向无纸化电子签署方式的转变，随之而来的是电子签署中对签名人身份认证和签名密钥安全性问题。对此，设计一种用于柜面文书签署场景的不动产业务办理柜面无纸化签署系统，系统集成于不动产一窗受理平台中，由客户端服务器、身份认证服务器、协同服务器构成，实现无纸化签署相关服务功能。依据对系统中关键技术的研究，提出了一种基于 SM2 的协同签名方案。方案中融合了对签名人身份的认证，运用 PBE 基于口令的密钥算法思想和门限密码学密钥分割思想提升密钥安全性。实践表明，该系统能够实现不动产柜面无纸化文书签署，提升不动产柜面业务办理工作效率，并为不动产业务日后的线上化改革、服务融合提供了建设基础。

关键词：电子政务；不动产业务办理；文书签署；SM2 协同签名

Design and implementation of paperless signature system for real estate counters based on SM2

CAI Zhaowei[1], LIU Congjun[1,2], LIU Chao[3]

(1 School of Computer Science, Jiangsu University of Science and Technology, Zhenjiang Jiangsu 212003, China;
2 JiangsuKeDa Huifeng Technology Co Ltd, Zhenjiang Jiangsu 212003, China;
3 Zhenjiang Real Estate Registration and Trading Center, Zhenjiang Jiangsu 212003, China)

【Abstract】 In recent years, the popularization of e-government has led to the change from the manual signing method of over-the-counter documents to the paperless electronic signing method in the processing of real estate business, followed by the issue of the identity authentication of the signer and the security of the signature key in the electronic signature. In this regard, design a paperless signing system for handling real estate business in counter document signing scenarios. The system is integrated into the real estate one-window acceptance platform, and consists of a client server, an identity authentication server, and a collaboration server to achieve paperless. Sign related service functions. The key technologies in the system are studied, and a collaborative signature scheme based on SM2 is proposed. The scheme integrates the authentication of the signer's identity and uses the PBE password-based key algorithm idea and the threshold cryptography key segmentation idea to improve the encryption. key security. Practice has shown that the system can realize the signing of paperless documents at the real estate counter, improve the work efficiency of real estate counter business processing, and provide a construction foundation for the online reform and service integration of real estate business in the future.

【Key words】 E-government; real estate business processing; document signing; SM2 co-signing

0 引 言

随着电子政务的不断发展及推广，为响应国务院办公厅《关于压缩不动产登记办理时间的通知》(国办发〔2019〕8 号)[1]精神，以及进一步提升省市“放管服”改革、“3550”改革和营商环境优化工作，各地不动产登记交易服务依次展开业务升级。其中不动产登记交易一窗受理平台[2]的搭建，给不动产业务带来更高的定位、更方便快捷的服务、更全面的服务融合、数据互联共享[3]等多方面提升。涉及到业务办理中的文书签署也被电子签署所取代[4]，不动产柜面业务办理逐渐向线上或柜面无纸化办理模式转变。

电子签署中所使用的公钥密码算法的密钥对由

作者简介：蔡昭炜(1994-)，男，硕士研究生，主要研究方向：信息安全、智能信息处理；刘从军(1968-)，男，硕士，高级实验师，硕士生导师，主要研究方向：智能信息处理、信息安全、云计算。

通讯作者：刘从军 Email：391986831@qq.com

收稿日期：2022-09-16

公钥和私钥组成。公钥由私钥进行不可逆计算得出，公钥对外公开，私钥需要秘密保存[5]。协同签名基于门限密码学思想提出，是一种需要多方参与才能完成签名、解密运算的数字签名技术。将签名密钥分割并存储于不同存储介质中[6]，可以增加攻击、破解密钥的难度同时减少密钥泄露的可能性。2017 年 Yehuda Lindell[7] 设计了一种快速安全的两方 ECDSA 签名方案。该方案运用 Paillier 的同态加密特性，并用零知识证明了方案的安全性，方案具有较好的性能。2020 年 Yudi Zhang 等人[8] 提出了一种可证明的、安全实用的两方分布式 SM2 签名算法协议，针对发展迅速的物联网移动端场景，能够在不需要重建私钥的情况下生成有效签名。2020 年冯琦等人[9] 设计了一种轻量级的非平衡 SM2 协同签名方案，方案中服务器协同客户端完成签名，过程中不暴露密钥信息。

在柜面签署场景下，签名人签署行为的真实性、文书签署行为所产生的签名是否表明签名人的真实意愿，是关注的重点。随着手工签署文书方式向线上电子签署方式的转变，该问题也随之转变为对签名者身份的核验以及签名所使用密钥的安全保护[10]。本文考虑上述存在的问题，提出一种用于不动产柜面签署场景的不动产业务办理柜面无纸化签署系统，并基于系统设计一种基于 SM2 的协同签名方案，用于生成不动产文书签名。方案在流程中引入签署人身份认证，使得签名能够表明签名人真实签名意愿，结合 PBE 基于口令的密钥算法思想，保护客户端私钥分量，并运用门限密码学思想，将密钥分散在客户端服务器和协同服务器中分别保存，以提高签名密钥安全性。

1　相关知识

1.1　SM2 数字签名算法

SM2 数字签名算法[11] 由国家密码管理局发布，是椭圆曲线公钥密码算法(SM)标准。在 SM2 数字签名算法中，通常采用 SM3 密码杂凑算法[12] 计算摘要。具体签名步骤如下：

(1)初始化：选定椭圆曲线参数 (q,a,b,G,n) 并输出；

(2)签名生成：选取私钥 d，计算 $P=[d]G$，将 P 作为公钥，由此得到密钥对 (P,d)；

(3)签名算法：设待签名消息为 M，签名者 A 生成消息签名需进行如下运算。

①计算杂凑值

$Z=H_{256}(ENTL_A \parallel ID_A \parallel a \parallel b \parallel x_G \parallel y_G \parallel x \parallel y)$

其中，ID_A 是长度为 *entlen Abit* 的可辨识标识；$ENTL_A$ 是 *entlenA* 转换而成的两个字节；(x_G,y_G) 是基点 G 的坐标；(x,y) 是公钥 P 的坐标。

计算 $e=H(\overline{M})$，其中 $\overline{M}=Z \parallel M$。

②使用随机数发生器产生 k，满足 $k \in [1,n-1]$；计算椭圆曲线点 $(x_1,y_1)=[k]G$。

③计算 $r=(e+x_1) \bmod n$。如果 $r=0$ 或 $r+k=n$，则返回上一步。

④利用私钥 d_A 和 r 计算

$s=(1+d)^{-1}(k-rd) \bmod n$。

⑤输出消息 M 的签名 (r,s)。

(4)验证算法：验证者收到签名者的签名 (r,s) 和明文 M 后，利用公钥 P 进行如下验证：

①计算 $e'=H(\overline{M'})$，其中 $\overline{M'}=Z \parallel M'$。

②计算 $t=(r'+s') \bmod n$，其中 (r',s') 即接收者 B 接收到的签名 (r,s)。如果 $t=0$，则直接返回验证失败。

③计算 $(x',y')=[s']G+(r'+s')P$。

④计算 $R=(e+x') \bmod n$

验证 $R=r'$ 是否成立，如果成立则返回验证成功，反之验证失败。

1.2　PBE 基于口令的密钥

PBE 是一种根据口令生成密钥来加密的方法[13]，在其生成密钥过程中，会通过伪随机数生成器生成一个被称为“盐”的随机数，与口令一起进行密钥计算，该方法可以有效防御字典攻击，其密钥生成过程如图 1 所示：

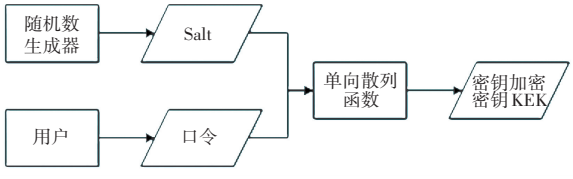

图 1　生成 PBE 密钥

Fig. 1　PBE key generation process

2　系统设计

2.1　系统硬件设计

系统硬件设计如图 2 所示。整体系统可以分为两部分，首先不动产业务办理柜面签署系统的业务模块集成在不动产一窗受理平台中，业务服务器与柜面工作 PC 设备相连并置于内网之中，柜面工作人员可以在业务系统中受理业务，推送任务到不动产一窗受理平台的各个子系统中。

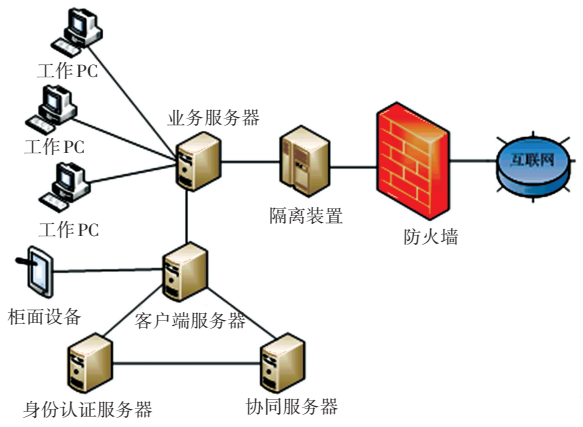

图 2 系统硬件设计

Fig. 2 System hardware design

不动产业务办理柜面签署系统的签署模块与业务服务器相连,由客户端服务器、身份认证服务器、协同服务器相连构成子系统,同时客户端服务器与不动产业务办理柜面签署设备连接。客户端服务器与协同服务器是实现数字签名运算的重要组成部分,身份认证服务器提供了对用户身份的核验甄别服务。本文基于这 3 个服务器,设计了一种基于 SM2 的协同签名方案,将签名密钥分割,在未来对不动产业务升级远程不见面签署服务[14]时,可以实现服务器的复用。

2.2 系统流程设计

不动产业务办理柜面签署系统的流程设计如图 3 所示。可以根据上述硬件设计的划分模式将整体流程划分为两部分。

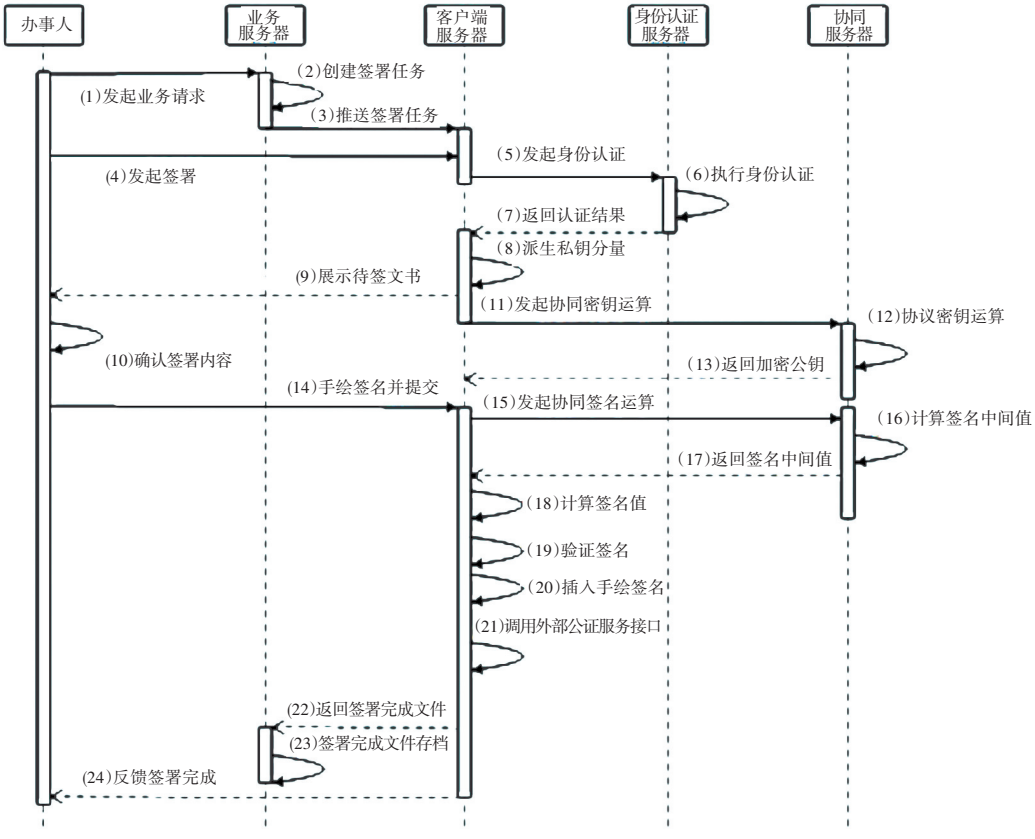

图 3 系统流程

Fig. 3 System process design

第一部分由用户发起业务申请开始。柜面工作人员在业务系统中根据用户需要办理的业务类型创建签署任务,并登记必要信息,业务系统会提取业务信息创建待签文书模板、生成用户口令 *Pin*。业务系统最终将签署任务及签署必要数据推送至客户端服务器中,等待用户唤醒。

第二部分由用户发起签署开始。用户使用柜面签署设备进行身份认证,身份认证成功后唤醒对应签署任务,此时客户端服务器将待签文书展示于柜面签署设备中,并派生客户端私钥分量与协同服务器进行协同密钥运算,计算用户密钥对。当用户确认待签文书无误并手绘签名提交后,客户端服务器

将与协同服务器协同运算，输出对文书的数字签名。客户端服务器验证签名通过后，将输出数据及手绘签名图样合成至待签文书中，得到已签署文书并返回至业务服务器。

3　基于 SM2 的协同签名方案设计

为实现不动产业务办理柜面无纸化签署系统中的不动产文书签名服务功能，设计了一种基于 SM2 的协同签名方案。

3.1　方案流程设计

方案的参与者包括：客户端 U（用户）、身份认证服务器 IS、协同服务器 CS。其中，身份认证服务器存储了代表 IS 身份的公私钥对（P_{IS}，K_{IS}），并通过安全信道将公钥 P_{IS} 发送至客户端 U 和协同服务器 CS。方案主要功能包括用户身份验证、协同密钥生成、签名生成。方案实现步骤如下：

（1）客户端将用户面部识别及 id 等数据发送到身份认证服务器（IS）进行身份认证。

（2）IS 向客户端 U 和协同服务器（CS）返回认证结果。

（3）客户端 U 使用用户口令及身份认证信息派生私钥分量。

（4）客户端 U 与 CS 协同计算公钥 P。

（5）客户端 U 与 CS 共同等待签署的文书运算数字签名 σ。

3.2　用户身份认证

用户身份认证主要由客户端和身份认证服务器协作完成。具体流程如下：

（1）柜面业务系统根据用户申报信息创建签署任务、生成用户口令 Pin，并推送至柜面签署设备（客户端 U）中。用户使用客户端，通过活体面部识别采集面部信息 f_u，使用 P_{IS} 加密面部信息 f_u、签名任务流水号 id_{task} 和用户 id，并向身份认证服务器 IS 发送认证请求 $Req_{ver}(Enc_{P_{IS}}(id, f_u, id_{task}))$。

（2）IS 收到认证申请后，使用私钥 K_{IS} 解密，将获得的用户 id 和面部信息 f_u 与公安公民身份信息库进行比对，并生成比对结果 f_v。

3.3　认证结果通知

IS 根据认证结果向客户端 U 和协同服务器 CS 反馈认证通知，若认证不通过，通知客户端 U 和协同服务器 CS 终止签署，若认证通过则会进行如下操作：

（1）IS 使用单项散列函数计算 $H(id \parallel id_{task} \parallel f_v)$。

（2）以 $H(id \parallel id_{task} \parallel f_v)$ 为消息，使用私钥 K_{IS} 对其计算签名 $Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$。

（3）将 $H(id \parallel id_{task} \parallel f_v)$、$Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$ 发送给客户端 U 及协同服务器 CS。

客户端和协同服务器使用 P_{IS} 验证签名 $Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$，若验证成功继续签署流程，否则终止签署。

3.4　客户端生成私钥分量

客户端 U 验证 $Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$ 成功，即用户身份验证成功后，需要完成签名前的准备工作：选定 SM2 椭圆曲线参数生成椭圆曲线；计算自身的密钥分量。具体实现过程如下：

（1）选取椭圆曲线 E，方程为 $y^2 = x^3 + ax + b$，其中 $a, b \in F_q$ 且满足 $4a^3 + 27b^2 \neq 0$。选择 E 上阶为 n 的基点 $G = (x_G, y_G)$，n 为大于 2 160 的素数；选取消息长度为 v 比特的 Hash 函数 H_v；选取输出为 256 b 比特串的 Hash 函数 $H_{256}: \{0,1\} \rightarrow Z_G$。

（2）将用户口令 Pin 视为 PBE 算法中的“盐”，与 $Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$ 共同作为参数输入到密钥派生算法中，生成一个符合 SM2 密码算法规则的密钥字符串 d_u。

3.5　协同密钥生成

协同密钥由客户端 U 和协同服务器 CS 共同生成，实现过程如下：

（1）客户端 U 使用密钥字符串 d_U 作为私钥分量，并计算 $P_u = [d_u]G$，将 P_u 发送给协同服务器 CS。

（2）协同服务器 CS 接收到 P_u 后，生成随机数 d_c，并计算 $P = [d_c]P_U - G$，P 作为公钥公开。

3.6　协同签名生成

如图 4 所示，用户在客户端 U 查阅文书并手绘签名后，将与协同服务器 CS 进行签名运算，生成数字签名 σ。具体运算步骤如下：

（1）客户端 U 计算用户杂凑值：$Z_u = H_{256}(ENTL_U \parallel ID_U \parallel a \parallel b \parallel x_G \parallel y_G \parallel x_p \parallel y_p)$，置 $\overline{M} = Z_A \parallel M$，其中 M 为待签名的文书。计算 $e = H_v(\overline{M})$。

（2）客户端使用随机数发生器生成随机数 $k_1 \in [1, n-1]$，计算变量 $Q_1 = [k_1]G$，将 Q_1、e 发送给协同服务器 CS。

（3）CS 使用随机数发生器生成两个随机数 k_2、$k_3 \in [1, n-1]$，计算变量 $Q_2 = k_2^{-1} Q_1$ 和椭圆曲线点 $(x, y) = k_3 G + k_3 Q_2$。

（4）CS 计算 $r = (e + x) \bmod n$，使用 r 计算签名

分量 $S_1 = d_c^{-1}\ k_2^{-1}\ k_3 \bmod n$ 和签名分量 $S_2 = d_c^{-1}(r + k_3) \bmod n$ 后，将 r、S_1、S_2 发送到客户端 U。

(5)客户端 U 收到 CS 发送的 r、S_1、S_2 后，计算签名 $S = d_u^{-1}\ k_1\ S_1 + d_u^{-1}\ S_2 - r \bmod n$，得到签名 $\sigma = (r,S)$。

(6)客户端 U 使用公钥 $P = [d_c]\ P_U - G$ 验证签名 σ，如果验证成功则输出签名 $\sigma = (r,S)$

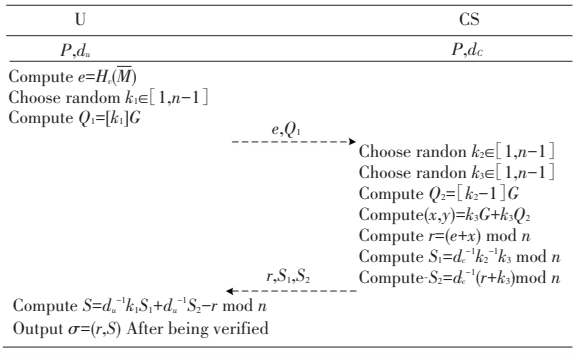

图 4 签名运算过程

Fig. 4 Signature calculation process

3.7 正确性分析

3.7.1 签名生成的正确性

协同密钥由 $P = [d_c]\ P_U - G$ 生成，则有：

$P = [d_c]\ P_U - G = d_c\ d_u G - G = (d_c\ d_u - 1)G$

协同服务器 CS 计算签名分量为：

$$S_1 = d_c^{-1}\ k_2^{-1}\ k_3 \bmod n$$

$$S_2 = d_c^{-1}(r + k_3) \bmod n$$

根据客户端 U 计算签名 S 可得：

$$S = d_u^{-1}\ k_1\ S_1 + d_u^{-1}\ S_2 - r\ mod\ n =$$

$$d_u^{-1}\ k_1\ d_c^{-1}\ k_2^{-1}\ k_3 + d_u^{-1}\ d_c^{-1}(r + k_3) - r\ mod\ n =$$

$$(d_u\ d_c)^{-1}\left[k_1\ k_2^{-1}\ k_3 + k_3 - r(d_u\ d_c - 1)\right] mod\ n =$$

$$[(d_u\ d_c - 1) + 1]^{-1}[k_1\ k_2^{-1}\ k_3 + k_3 -$$

$$r(d_u\ d_c - 1)]\ mod\ n$$

此时，可设签名 $\sigma = (r,S)$ 是由私钥 $d = d_u\ d_c - 1 \bmod n$ 和随机数 $k = k_1\ k_2^{-1}\ k_3 + k_3 \bmod n$ 生成的 SM2 签名，满足 $S = (1 - d)^{-1}(k - rd) \bmod n$。因此，方案生成的签名 $\sigma = (r,S)$ 是正确的。

3.7.2 签名验证的正确性

根据客户端 U 计算椭圆曲线点 (x,y)：

$$(x,y) = k_3 G + k_3 Q_2 = k_3 G + k_3\ k_1\ k_2^{-1} G = (k_1\ k_2^{-1}\ k_3 + k_3)\ G$$

验证者想要验证签名，需要使用收到的签名 $\sigma = (r',S')$ 和公钥 P，计算椭圆曲线点 $(x',y') = [S']G + (r' + S')P$，则有：

$$(x',y') = [S']\ G + (r' + S')\ P =$$

$$[1 + (d_u\ d_c - 1)]^{-1}[(k_1\ k_2^{-1}\ k_3 + k_3 -$$

$$r(d_u\ d_c - 1)]G + r'P + S'P =$$

$$\frac{(k_1\ k_2^{-1}\ k_3 + k_3)\ G + (k_1\ k_2^{-1}\ k_3 + k_3)\ P}{1 + (d_u\ d_c - 1)} =$$

$$\frac{[1 + (d_u\ d_c - 1)]\ (k_1\ k_2^{-1}\ k_3 + k_3)\ G}{1 + (d_u\ d_c - 1)} =$$

$$(k_1\ k_2^{-1}\ k_3 + k_3)\ G = (x,y)$$

如果签名 $\sigma = (r,S)$ 正确，从上式可以得知 $x = x'$，验证者只需要通过计算 $R = (e + x') \bmod n$ 和 r 是否相等来判断签名验证是否成功。

4 实验测试

为验证方案，搭建了硬件环境进行实验测试，硬件参数配置见表 1。

表 1 硬件参数

Tab. 1 Hardware parameters

设备类型	配置参数
客户端	CPU：8 核 1.8 GHz RAM 容量：12 GB
身份认证服务器	操作系统：Windows 10 CPU：Intel(R)Corei7-7700 RAM 容量：16 GB
协同服务器	操作系统：CentOS CPU：Intel(R)Corei5-9400 RAM 容量：16 GB

程序构建基于 bcprov-jdk 加密解密库，主要通过业务模拟的方式对系统进行功能测试，同时在测试中对采用的 SM2 协同签名方案进行耗时记录，用于性能分析。

4.1 功能测试

根据业务流程设计，签署任务需要在创建阶段采集必要的业务信息，其中包括业务类型、不动产登记信息、办理人身份资料等。合同文书签署模板需要根据这些必要信息进行创建，并推送至客户端服务器开始签署。

签署任务推送至客户端服务器后，用户使用柜面设备进行业务办理，柜面设备签署界面如图 5 所示，用户确认签署并手绘签名后，系统进行签名运算，生成签名后客户端服务器会对所生成签名进行验证。若验证通过，则合成并输出如图 6 所示的已签署文书。

图 5　柜面设备签署界面

Fig. 5　Counter equipment signing interface

图 6　合成后的已签署文书示例

Fig. 6　Example of signed instrument

4.2　性能测试

图 7 反映了本文 SM2 协同签名方案各阶段的性能表现。在身份认证阶段主要考虑身份认证服务器 IS 生成服务器签名 $Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$ 的耗时，认证通知阶段主要考虑客户端 U 和协同服务器 CS 对 $Sign_{IS}(H(id \parallel id_{task} \parallel f_v))$ 的验证耗时。

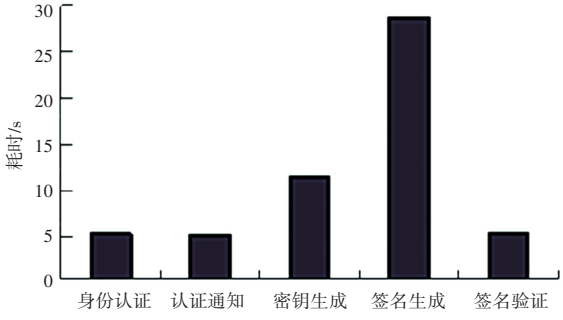

图 7　本文方案各阶段运算耗时

Fig. 7　Operation time consumed in each stage

图 8 展示在密钥生成阶段、签名生成阶段客户端服务器与协同服务器的耗时情况，同时将两者与原始 SM2 数字签名方案的性能表现进行对比。

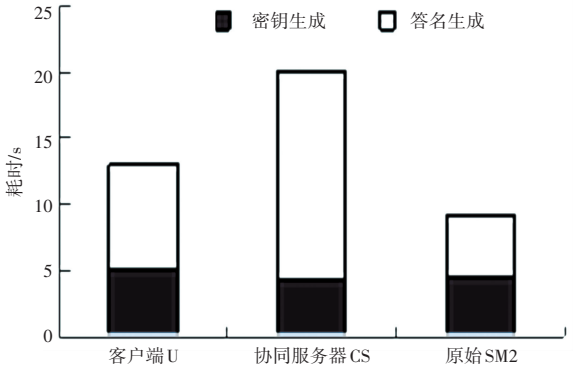

图 8　密钥、签名生成性能对比

Fig. 8　Comparison of key and signature generation performance

总体来看，本文方案在密钥生成阶段客户端及协同服务器性能表现接近原始 SM2 签名方案，在具有更好性能的服务器架构中，协同服务器的签名运算速度能够进一步得到缩减。

将本文所提签名方案与文献[15]和文献[9]中提出的 SM2 协同签名方案进行计算效率对比，结果见表 2。定义 Exp 表示一次标量点乘运算或模幂运算，对于形如 $d_c^{-1}(r + k_3) = d_c^{-1}r + d_c^{-1}k_3$ 的多点乘法等同于一次点乘运算所需时间，加法运算所需计算量忽略不计。文献[9]方案中使用了零知识证明，但在半诚实模型下，通信双方诚实计算可以省略零知识证明，故在对比时只考虑在半诚实模型下的计算效率。

表 2　计算效率对比

Tab. 2　Calculation efficiency comparison

方案	通讯轮数	密钥生成		签名生成	
		参与方 A	参与方 B	参与方 A	参与方 B
文献[15]	3	1Exp	2Exp	3Exp	3Exp
本文	2	1Exp	1Exp	2Exp	4Exp
文献[9]	2	2Exp	1Exp	2Exp	3Exp

通过对比分析，本文方案只需要 2 轮通信，在密钥生成阶段通信双方都只需要 1Exp，总体优于文献[9]和文献[15]中所提方案。在签名生成阶段中，客户端服务器(参与方 A)需要 2Exp，优于文献[15]方案，将更多的计算消耗放在硬件性能更好的协同服务器(参与方 B)中，转移了部分运算压力。由此可见，本文方案在计算效率上具有较好表现。

图 9 展现了不动产业务办理柜面无纸化签署系统与手工文书签署的在不同业务数量下平均工作效率对比结果。

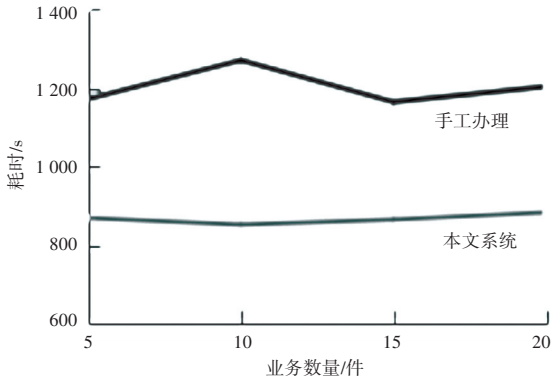

图 9 业务办理效率对比

Fig. 9 Comparison of business handling efficiency

在实际调研中发现,不动产柜面业务办理手工文书签署方式在材料、文书的核实、打印、整理、收纳上耗费大量的时间和沟通成本,导致柜面工作效率无法提高。不动产业务办理柜面无纸化签署系统在实际使用在文书处理、保存上具有显著优势,不但缩短了业务办理时长,提高了柜面工作效率,同时也实现对合同文书的电子化归档和整合,规避了纸质文书归档保存时可能出现管理不善的风险。因此,本方案在柜面无纸化签署场景下具有良好的应用效果。

5 结束语

针对不动产柜面业务办理手工文书签署向柜面无纸化签署转变而带来的签名人身份认证和密钥安全问题,本文方案提出了一种不动产业务办理柜面无纸化系统,在系统设计中考虑了后续不动产业务升级优化预留了兼容空间,并根据系统设计了一种基于 SM2 的协同签名方法,在方案流程融入了身份认证服务,采用门限密码学思想将签名所需要的密钥分割在客户端及协同服务器中,提高了密钥存储的安全性。此外,方案结合 PBE 基于口令密钥算法的思想,提升了客户端私钥分量的安全性,在实际场景中具有良好的应用效果。

由于不动产登记交易业务的特殊性,未来研究方向是将电子公证技术与系统进行融合升级,提升电子文书法律效力,减少办理人业务办理成本。

参考文献

[1] 国务院办公厅关于压缩不动产登记办理时间的通知[J]. 中华人民共和国国务院公报,2019,1656(9):39-41.
[2] 商桂华. 不动产登记"一窗受理"实施的必要性及对策探析[J]. 住宅与房地产,2021,600(3):19-20.
[3] 徐晗. 不动产登记一窗受理数据共享系统设计与实现[D]. 江苏:江苏科技大学,2019.
[4] 王海涛. 论数字签名在电子政务中的应用[J]. 旅游纵览,2012(10):151.
[5] 赵臻,吴戈,赖建昌,等. 公钥密码方案构造及安全证明的知识要点和方法论[J]. 密码学报,2019,6(1) : 1-17.
[6] 廖会敏,王栋,玄佳兴,等. 基于国产公钥密码算法的门限签名及解密方案[J]. 计算机应用与软件,2021,38(6):313-317.
[7] LINDELL Y. Fast Secure Two-Party ECDSA Signing[C]// Annual International Cryptology Conference. Springer, Cham, 2017:613-644.
[8] YUDI ZHANG, DEBIAO HE, MINGWU ZHANG, et al. A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm[J]. Frontiers of Computer Science,2020,14(3):196-208.
[9] 冯琦,何德彪,罗敏,等. 移动互联网环境下轻量级 SM2 两方协同签名[J]. 计算机研究与发展,2020,57(10):2136-2146.
[10] 蔡京露,王文昌. 电子合同签署系统[J]. 信息技术与标准化,2018,405(9):77-80.
[11] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会.信息安全技术 SM 椭圆曲线公钥密码算法第 2 部分:数字签名算法:GB/T 32918.2-2016[S]. 2016.
[12] 谢宗晓,甄杰,董坤祥. 国产商用密码算法 SM3 及其相关标准介绍[J]. 中国质量与标准导报,2021,275(3):14-16.
[13] 咸凛,郝嘉. 一种基于 PUF 的 PBE 系统[J]. 通信技术,2019,52(5):1224-1227.
[14] 赵宏伟. 政务服务"网上办、不见面"是应对突发疫情的必然选择[J]. 公共管理评论,2020,2(2):144-148.
[15] 苏吟雪,田海博. 基于 SM2 的双方共同签名协议及其应用[J]. 计算机学报,2020,43(4):701-710.

(上接第 121 页)

[7] 黄胜,冉浩杉. 基于语义信息的精细化边缘检测方法[J]. 计算机工程, 2022, 48(3): 204-210.
[8] 刘晓君,韩芳,赵磊. 一种改进的 SAR 影像边缘检测方法[J]. 测绘通报, 2017, 486(9): 56-59.
[9] 刘丽霞,李宝文,王阳萍,等. 改进 Canny 边缘检测的遥感影像分割[J]. 计算机工程与应用, 2019, 55(12): 54-58, 180.
[10] 陈顺,孟青青,李登峰. 结合图像增强和改进 Canny 算子的遥感图像边缘检测[J]. 河南大学学报(自然科学版), 2020, 50(5): 623-630.
[11] 马为駧,张奘,马传香,等. 不同光照条件下含噪遥感图像边缘检测算法[J]. 吉林大学学报(工学版),2023, 53(1): 241-247.
[12] 方政,胡晓辉,陈永. 基于多方向中值滤波的各向异性扩散滤波算法[J]. 计算机工程与应用, 2017, 53(4): 195-199.
[13] 卞艳,宫雨生,马国鹏,等. 基于无人机遥感影像的水体提取方法[J]. 浙江大学学报(工学版), 2022, 56(4): 764-774.
[14] 陈思吉,王晓红,李运川. 改进 Laplace 的无人机图像边缘检测算法研究[J]. 测绘工程, 2021, 30(2): 36-44.
[15] 黄巍,黄辉先,徐建闽,等. 基于 Canny 边缘检测思想的改进遥感影像道路提取方法[J]. 国土资源遥感, 2019, 31(1): 65-70.
[16] 刘宇涵,闫河,陈早早,等. 强噪声下自适应 Canny 算子边缘检测[J]. 光学精密工程, 2022, 30(3): 350-362.